Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key corresponding to a symmetric algorithm and encrypting said media key with a public key of a compliant playing device;

(b) delivering said media data set, media key encrypted in the step (a), a media certificate, and a key renewing certificate to said playing device, said media certificate being required to recognize by said playing device a valid private key among a plurality of private keys stored in said playing device and including a private-key identification and media identification of said playing device, said private-key identification being generated by encrypting said media identification with said public key of said playing device, wherein said key renewing certificate is required to update a private key of said playing device and including a pair of new public key and private key of said playing device and a time mark for sequencing said public and private keys from the oldest to the newest, respectively;

(c) searching for an actual private key using said private-key identification and said media identification;

(d) decrypting said delivered media key with said actual private key; and

(e) decrypting said delivered media data set with said decrypted media key;

(f) processing said key renewing certificate using a master private key of said playing device~~, wherein said master key is encrypted with a current public key of said playing device~~, and analyzing said time mark; ~~and~~

(g) replacing a pair of current public and private keys of said playing device with said pair of new public and private keys if said key renewing certificate is the newest one as a result of analysis; and

(h) encrypting said master private key with said new public key of said playing device.

2. (Original) The method of claim 1, wherein said stored private keys include said current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

3. (Original) The method of claim 2, wherein said playing device includes a rewritable memory storing said old private keys.

4. (Previously Presented) The method of claim 3, wherein said old private keys being stored in said memory are encrypted with said public key.

5. (Currently Amended) A copy protection system for digital media, the system comprising:

a private key verifier configured to receive a media certificate and a key renewing certificate, said media certificate including a private-key identification of a compliant playing device and searching for an actual private key by checking whether each of available private keys of said playing device corresponds to said private-key identification, wherein said media certificate is required to recognize by said ~~play~~ playing device the actual private key among a plurality of private keys stored in said playing device, wherein said key renewing certificate is required to update a private key of said playing device and includes a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively, wherein said key renewing certificate is required to update a private key of said playing device;

a media key decryptor configured to receive an encrypted media key and decrypting said media key with said actual private key;

a media data decryptor configured to receive an encrypted media data set and decrypt said media data set with said decrypted media key; and

a processor configured to process said key renewing certificate using a master private key of said playing device~~, wherein said master key is encrypted with a current public key of said playing device~~, analyze the time mark, ~~and~~ replace a pair of current public and private keys of said playing device with said pair of new public and private keys if said key renewing certificate is the newest one as a result of the analysis, and encrypt said master private key with said new public key of said playing device.

6. (Previously Presented) The system of claim 5, wherein said available private keys include said current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

7. (Currently Amended) The system of claim 6, further comprising a data-rewritable memory ~~storing~~ configured to store said one or more old private keys.

8. (Previously Presented) The system of claim 7, where said old private keys being stored in said memory are encrypted with a public key of said playing device.

9. (Original) The system of claim 5, wherein said encrypted media key is encrypted with a public key of said playing device.

10. (Original) The system of claim 5, wherein said encrypted media data set is encrypted with an original media key.

11. (Currently Amended) A copy protection method for digital media, the method comprising:

(a) encrypting an original media data set with a media key and encrypting said media key with a public key of a compliant playing device;

(b) delivering the encrypted media data set, the encrypted media key a media certificate, and a key renewing certificate to said playing device, the media certificate being required to recognize by said playing device a valid private key among a plurality of private keys stored in said playing device, wherein said key renewing certificate is required to update a private key of said playing device and including a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively;

(c) identifying the valid private key among private keys stored in said playing device in response to said media certificate;

(d) decrypting said delivered media key with the valid private key identified as a result of the step (c);

(e) decrypting said delivered media data set with said decrypted media key;

(f) processing said key renewing certificate using a master private key of said playing device~~, wherein said master key is encrypted with a current public key of said playing device~~, and analyzing the time mark; ~~and~~

(g) replacing a pair of current public and private keys of said playing device with said pair of new public and private keys if said key renewing certificate is the newest one as a result of analysis; and

(h) encrypting said master private key with said new public key of said playing device.

12. (Previously Presented) The method of claim 11, wherein said stored private keys include said current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

13. (Previously Presented) The method of claim 11, further comprising:

not permitting a playback of the media data set when the valid private key is not identified as a result of step (c).

14. (Currently Amended) A copy protection method for digital media, the method comprising:

(a) receiving an encrypted media data set, an encrypted media key, a media certificate, and a key renewing certificate, wherein said encrypted media set is generated by encrypting an original media data set with a media key, said encrypted media key is generated by encrypting said media key with a public key of a compliant playing device, and said media certificate is required to recognize a valid private key among a plurality of private keys stored in said playing device, wherein said key renewing certificate is required to update a private key of said playing device and includes a pair of new public key and private key of said playing device and a time mark for sequencing the public and private keys from the oldest to the newest, respectively;

(b) identifying the valid private key among each of stored private keys of said playing device in response to said media certificate; and

(c) decrypting said received media key with the valid private key identified by the step (b), and decrypting said received media data set with said decrypted media key;

(d) processing said key renewing certificate using a master private key of said playing device, ~~wherein said master key is encrypted with a current public key of said playing device;~~ and analyzing the time mark; ~~and~~

(e) replacing a pair of current public and private keys of said playing device with said pair of new public and private keys if said key renewing certificate is the newest one as a result of said analyzing; and

(f) encrypting said master private key with said new public key of said playing device.

15. (Previously Presented) The method of claim 14, wherein said stored, private keys include said current private key and one or more old private keys, each of said old private keys being previously revoked through a key revocation process.

16. (Previously Presented) The method of claim 14, further comprising:

not permitting a playback of the media data set when the valid private key is not identified as a result of step (b).

17. (Canceled)

18. (Previously Presented) The method of claim 14, wherein the previous private key is included in a private key history and database when replacing the keys as a result of step (e).

19. (Currently Amended) The method of claim 1, wherein, in step (b), said pair of new public and private keys are encrypted with a master public key of said playing device and delivered to said playing device.

20.-21. (Canceled)

22. (New) The method of claim 1, wherein step (f) comprises decrypting an encrypted master private key with said current private key of said playing device into said master private key.

23. (New) The system of claim 5, wherein said key verifier is configured to receive said pair of new public and private keys encrypted with a master public key of said playing device.

24. (New) The system of claim 5, wherein said processor comprises a master key decryptor configured to decrypt an encrypted master private key with said current private key of said playing device into said master private key.

25. (New) The method of claim 11, wherein, in step (b), said pair of new public and private keys are encrypted with a master public key of said playing device and delivered to said playing device.

26. (New) The method of claim 11, wherein step (f) comprises decrypting an encrypted

master private key with said current private key of said playing device into said master private key.

27. (New) The method of claim 14, wherein, in step (a), said received pair of new public and private keys is encrypted with a master public key of said playing device.

28. (New) The method of claim 14, wherein step (d) comprises decrypting an encrypted master private key with said current private key of said playing device into said master private key.